(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－269957
（P2000－269957A）
(43)公開日　平成12年９月29日(2000.9.29)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	５Ｂ０４９
Ｇ０６Ｆ　19/00		Ｇ０９Ｃ　1/00	６２０Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６２０		６４０Ｂ	９Ａ００１
	６４０	Ｇ０６Ｆ　15/28	Ｂ	

審査請求　未請求　請求項の数11　ＯＬ　（全８頁）

(21)出願番号　特願平11－73118

(22)出願日　平成11年３月18日(1999.3.18)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　相馬　浩之
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　田中　博樹
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

最終頁に続く

(54)【発明の名称】　電子投票方法及びそのプログラム記録媒体

(57)【要約】
【課題】　投票者以外の者に、投票者名と投票内容の対応を隠蔽する。
【解決手段】　開票者は公開鍵暗号の暗号鍵と復号鍵を生成し（Ｓ１）、暗号鍵を全ての投票者に配布し（Ｓ２）、投票者は投票ＩＤの発行を認証者に行い（Ｓ３）、認証者は投票ＩＤを投票者に発行し（Ｓ４）、投票者は投票内容を暗号鍵で暗号化し（Ｓ６）、その暗号化票と投票ＩＤを認証者へ送り（Ｓ７）、認証者はその票の正当性を認証し（Ｓ８）、その暗号化票と投票ＩＤのリストを開票者へ送り（Ｓ１１）、開票者は暗号化票を復号鍵で復号して、投票の集計を行い、投票ＩＤを合せて、投票結果を公開する（Ｓ１３）。

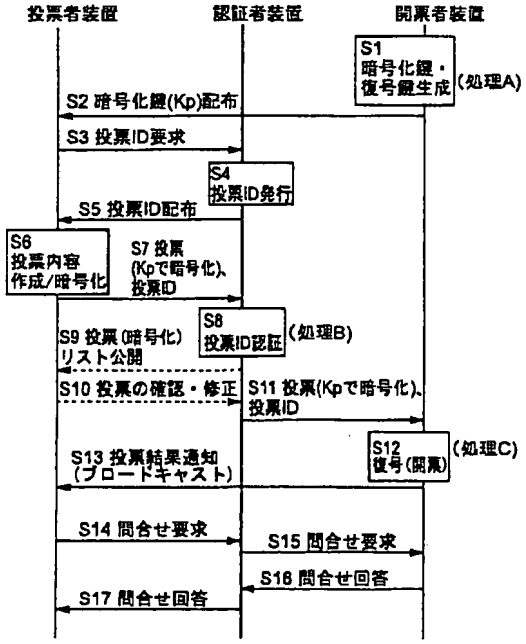

図１

1

【特許請求の範囲】

【請求項１】　ネットワークを用いた電子投票方法において、

投票者装置は票を認証者装置へ送り、

認証者装置はその投票者が本人であること、その票が投票者本人によるものであること、票が重複して投じられていないことを確認し、

その確認に全て合格するとその票を開票者装置へ送り、

開票者装置は受信した票を開票することを特徴とする電子投票方法。

【請求項２】　請求項１記載の電子投票方法において、

開票者装置は公開鍵暗号方式の暗号化鍵と復号鍵を生成し、その暗号化鍵を投票者装置へ配布し、

投票者装置は票を暗号化して認証者装置へ送り、

開票者装置は暗号化票を復号鍵で復号して開票することを特徴とする電子投票方法。

【請求項３】　請求項１又は２記載の電子投票方法において、

投票者装置は認証者装置に投票ＩＤの発行を要求し、

認証者装置はその発行要求に応答して投票ＩＤを発行して利用者装置へ配布し、

投票者装置は認証者装置へ送る票に投票ＩＤを付加し、

認証者装置は開票者装置へ送る票に投票ＩＤを付加し、

開票者装置は開票集計した票と対応する投票ＩＤとの関係を投票結果として投票者装置に公開することを特徴とする電子投票方法。

【請求項４】　請求項１乃至３の何れかに記載の電子投票方法において、

投票者装置は氏名、年令、性別などの個人情報を票に付加して送信し、

認証者装置は個人情報中の公開してよいものを票に付けて開票者装置へ送ることを特徴とする電子投票方法。

【請求項５】　投票者装置が投票を認証者装置を介して開票者装置に行うネットワークを用いる電子投票方法における投票者装置のコンピュータが、

投票ＩＤの発行要求を認証者装置に行う処理と、

認証者装置から投票ＩＤを取得する処理と、

投票内容を作成し、その投票内容を暗号化して票を作成する処理と、

その票を認証者装置へ送る処理と、

認証者装置から投票内容確認要求を受信する処理と、

投票内容に変更があると再び票の作成処理を行う処理と、

投票内容に変更がないと投票内容確認回答を認証者装置へ送る処理とを実行させるプログラムを記録した記録媒体。

【請求項６】　投票者装置が投票を認証者装置を介して開票者装置に行うネットワークを用いる電子投票方法における認証者装置のコンピュータに、

投票者装置から投票ＩＤ発行要求を受信する処理と、

2

投票ＩＤを発行する処理と、

発行した投票ＩＤを投票者装置へ送信する処理と、

投票者装置から票と投票ＩＤと認証書を受信する処理と、

受信した票の正当性を認証する処理と、

受信した認証書を用いて投票者の本人性を認証する処理と、

受信した票が真の投票者によりなされたかを認証する処理と、

受信した票が二重投票でないことの認証をする処理と、

投票期限内に受信した票を収集しリストを作成する処理と、

その投票リストを開票者装置へ送る処理とを実行させるプログラムを記録した記録媒体。

【請求項７】　請求項６記載の記録媒体において、

上記正当性を認証する処理は受信した認証書を用いて投票者の本人性を認証する処理と、

受信した票が真の投票者によりなされたかを認証する処理と、

受信した票が二重投票でないことの認証をする処理とよりなることを特徴とする記録媒体。

【請求項８】　請求項６又は７記載の記録媒体において、

投票者装置からの問合せ要求を受信する処理と、

受信した問合せ要求を開票者装置へ送信する処理と、

開票者装置から問合せ回答を受信する処理と、

受信した問合せ回答を投票者装置へ送信する処理と、

を上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項９】　請求項６乃至８の何れかに記載の記録媒体において、

上記正当性の認証処理の後に、投票内容の確認要求を投票者装置に行う処理と、

投票者装置から投票内容確認の回答を受信する処理とを上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項１０】　投票者装置が投票を認証者装置を介して開票者装置に行うネットワークを用いる電子投票方法における開票者装置のコンピュータに、

暗号化鍵、復号鍵の対を生成する処理と、

上記暗号化鍵を投票者装置に配布する処理と、

認証者装置から投票リストを取得する処理と、

投票リスト中の暗号化票を復号鍵で復号して票の集計を行う処理と、

集計した投票結果を公開する処理とを実行させるプログラムを記録した記録媒体。

【請求項１１】　請求項１０記載の記録媒体において、

認証者装置から問合せ要求を受信する処理と、

受信した問合せ要求に対する問合せ回答を認証者装置に送信する処理とを上記コンピュータに実行させるプログ

ラムを上記プログラムが含むことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ネットワークを介して電子投票を行う際に、投票者が開票者を含む投票者以外の者に対して投票者名と投票内容の対応を隠蔽できる電子投票方法及びそのプログラム記録媒体に関するものである。

【０００２】

【従来の技術】ネットワークを介して投票を行う電子投票が知られている。例えば、インターネット上で人気投票を実施する際に用いられている。ここで、電子投票において厳密性が求められる選挙などで利用する際に求められる要求条件は以下のとおりである。

【０００３】

１．有権者のみによる投票でなければならない
２．二重投票はできない
３．他人の投票内容を知ることはできない
４．他人の票を複製することはできない
５．誰かが投票内容に不正（改竄（かいざん）や消去）をした場合、それを発見することができなければならない
６．全ての投票者は、投票終了時に自身の票が有効であったかを確認できなければならない

これらを満たす電子投票方式としてＳｃｈｎｅｉｅｒの電子投票プロトコルがある。これは電子投票では投票者と開票者の２者間で行われる。投票者が投票する際、開票者が投票者の認証を行い、票の正当性を判断して開票を行い、その票内容を集計結果に反映させる手順をとっている。このとき、開票者は直接投票者から票を受け取るために、投票者名と投票内容の対応を把握できてしまう。その場合、投票者の投票内容がネットワーク上を流れることになるが、ネットワークを介して投票を行う投票者から、投票者自身の思想、意思などのプライベートな情報を他人に対して知られたくないという要求が挙げられている。

【０００４】図６に従来の電子投票方式を示す。図６では投票者と開票者の２者間で投票、認証、開票を行っている。まず投票者は、投票を行うために投票希望通知を開票者に送る（Ｓ１）。開票者は投票希望通知を発した投票者に対して、投票ＩＤを発行・配送する（Ｓ２，Ｓ３）、投票ＩＤを受け取った投票者は公開鍵／秘密鍵である鍵対を生成する（Ｓ４）。この鍵を用いて投票者は投票内容を作成・暗号化し（Ｓ５）、投票ＩＤとともに開票者へ配信する（Ｓ６）。それを受け取った開票者は、投票ＩＤの認証を行い（Ｓ７）、暗号化された投票のリストを作成し、投票者に公開する（Ｓ８）。投票者は、リストを確認し、修正などがあれば、改めて投票を行う（Ｓ９）。公開された投票内容で良ければ、投票者はその投票を開票するための復号鍵を投票ＩＤとともに配送する（Ｓ１０）。投票内容が決定した場合、特定期間経過後、開票者は復号して開票し（Ｓ１１）、投票の集計結果を投票者に対して公表する（Ｓ１２）。

【０００５】この方式の特徴を以下に示す。

１．有権者に対し投票ＩＤを与え、これを識別子として投票に対する権利を与える（処理Ｓ１，Ｓ２）。
２．投票ＩＤにより、投票回数をチェックする（処理Ｓ７）。
３．投票内容に対して、暗号化を施す（処理Ｓ４，Ｓ５）。

【０００６】４．デジタル署名と証明書を添付することにより、第３者からの攻撃を防止（処理Ｓ６，Ｓ９，Ｓ１０）。
５．投票ＩＤと投票者名をリストにして保持することにより、追跡が可能（処理Ｓ２）。
６．集計結果に投票ＩＤを呈示することにより、投票の正当性を開示する（処理Ｓ８，Ｓ１２）。

【０００７】

【発明が解決しようとする課題】従来の技術では、開票者が投票者名と投票内容の双方を入手できることに問題があった。つまり、開票者は投票者名と投票内容の対応を知ることができ、投票者に対してプライバシー保護を提供することができない。この発明は、投票者が何に対して投票をしたかを開票者を含む投票者以外の者から投票者名と投票内容の対応を隠蔽し、かつ二重投票や不正投票を防止・追跡する機能を有し、また投票者が自身の票が有効であったかを確認できる電子投票方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するための方法として、この発明においては投票者装置と開票者装置の間に投票者を認証しつつ、投票者名と投票内容の対応を分離する認証者装置を仲介者装置として設定する。また、認証者装置を設ける際に、認証者装置は投票者装置から票を受け取るため、認証者装置に対して投票内容を隠蔽する必要があり、投票内容に対して開票者装置にしか開票できないような暗号化を施す。この暗号化・復号鍵の生成は、開票者装置が行い、投票に対する暗号化は投票者装置自身が行うことにより、開票者を除く投票者以外の者から投票内容を隠蔽する。

【０００９】投票者装置は、開票者装置から投票に対して施す暗号化の鍵を受け取る。投票者装置は、認証者装置へ投票時に必要な投票ＩＤを取得するために、投票ＩＤ発行要求を送信し、その結果として投票ＩＤ発行回答を受信するとともに投票ＩＤを受け取る投票ＩＤ発行処理と、投票ＩＤを取得し、投票内容を作成し、暗号化処理を施し、認証者装置へ投票要求を送信し、認証者装置から投票回答を受信し、その後認証者装置へ暗号化した投票内容を投票ＩＤとともに送信し、認証者装置から投

票内容確認要求を受信し、変更がなければ認証者装置へ投票内容確認回答を送信する投票処理と、投票結果と自票の有効性を確認することができる投票結果通知処理と、投票結果に対して問合せを行う問合せ処理とをそれぞれ行う機能を有することを特徴とする。

【００１０】認証者装置は、投票者装置から投票ＩＤ発行要求を受け、投票ＩＤを発行して、その結果として投票ＩＤ発行回答を投票者装置へ送信する投票ＩＤ発行処理と、投票者装置から投票要求を受け、投票回答を返し、投票を受信し、その投票の正当性を確認する認証処理と、投票の内容確認要求を投票者装置へ送信し、投票者装置から投票内容確認回答を受信する投票処理と、投票を収集し、投票リストを作成して開票者装置へ投票リスト投入要求を送信し、開票者装置から投票リスト投入回答を受信し、開票者装置へ投票リスト配布を行う投票リスト投入処理と、投票者装置から問合せ要求を受け、開票者装置へ問合せ要求を送信し、開票者装置から問合せ回答を受信し、投票者装置へ問合せ回答を送信する問合せ処理とをそれぞれ行う機能を有することを特徴とする。

【００１１】開票者装置は、暗号化・復号鍵生成処理により生成した暗号化鍵を投票者装置へ配布する暗号化鍵配布処理と、認証者装置から投票リスト投入要求を受け、投票リスト投入回答を返し、投票リストを受け取る投票リスト投入処理と、投票リストを開票（復号）し、投票を集計し、投票結果を投票者装置へ配布する投票結果通知処理と、認証者装置から問合せ要求を受け、認証者装置へ問合せ回答を送信する問合せ処理とをそれぞれ行う機能を有することを特徴とする。

作用

投票者を認証する認証者装置を仲介者装置として設けることで、開票者装置は投票者名を判別できなくなり、その結果、投票者は開票者に対してプライバシーが保護される。

【００１２】また、認証者装置を設けた際、開票者装置が投票に対する暗号化鍵と復号鍵を生成する。ただし、暗号化方式として公開鍵暗号化方式を使うものとする。開票者装置はここで生成した暗号化鍵を事前に投票者装置へ配布し、復号鍵は秘密にしておく。これにより、投票者装置は投票内容に暗号化を施すことができ、開票者を除く投票者以外の者から投票内容の隠蔽が可能となる。

【００１３】

【発明の実施の形態】仲介者（認証者装置）を設け、投票内容を暗号化するための鍵を生成する装置を開票者装置としたこの発明の電子投票方法の概要を図１に示す。まず、開票者装置は公開鍵暗号での暗号化鍵（公開鍵）と復号鍵（秘密鍵）を生成し（Ｓ１）（処理Ａ）、暗号化鍵Ｋｐを投票者装置に配布する（Ｓ２）。投票者装置は認証者装置に、投票時に必要な投票ＩＤを要求し（Ｓ３）、認証者装置は投票ＩＤを発行して（Ｓ４）、投票者装置へ配布する（Ｓ５）。その投票ＩＤと投票者装置との対応を認証者装置に記憶しておく。

【００１４】投票者装置は開票者装置から入手した暗号化鍵Ｋｐを用いて投票内容を暗号化し（Ｓ６）、その暗号化投票と投票ＩＤを認証者装置へ配送する（Ｓ７）。これを受け取った認証者装置は投票者の認証を行い（Ｓ８）（処理Ｂ）、票の正当性を立証できれば開票者装置へ票とその投票ＩＤを転送する（Ｓ１１）。この際に必要に応じて認証者装置は暗号化投票のリストを投票者装置に公開し、投票内容の確認を要求し（Ｓ９）、投票者装置は投票内容の確認を行い、変更があれば改めて投票しなおす（Ｓ１０）。票を受け取った認証者装置は、復号鍵を持たないため不正に開票を行うことができない。認証者装置から投票者装置の投票を受け取った開票者装置は、復号鍵を用いて開票する（Ｓ１２）（処理Ｃ）。その開票結果は、ブロードキャストにより、全投票者装置へ通知される（Ｓ１３）（処理Ｄ）。投票者はその開票結果の投票した内容に自己の投票ＩＤが含まれていれば正しく開票されたことになり、自己の投票ＩＤが含まれていなければ、問合せ要求を認証者装置へ送り（Ｓ１４）、認証者装置はその問合せ要求を開票者装置へ送る（Ｓ１５）。開票者装置はその問合せに対する回答を認証者装置へ送り（Ｓ１６）、認証者装置はその問合せ回答を利用者装置へ送る（Ｓ１７）。

【００１５】図２にこの発明での投票プロセスにおける処理を示す。まず、暗号化鍵配布処理では、開票者装置が投票者装置に対して投票内容に暗号化を施すための暗号化鍵および復号鍵の生成を行う。ここで生成した暗号化鍵のみを投票者装置の全てに対して配布を行う。投票ＩＤ発行処理では、認証者装置が投票者装置に対して投票時に必要な投票ＩＤの発行・提供を行う。投票処理では、実際に票を投じる際に行われる。投票リスト投入処理では、認証者装置が収集した投票から作成した投票リストを開票者装置に対して提供する際に実行される。問合せ処理は、投票者装置が投票結果に対して問合せる際に実行される。

【００１６】図３にこの発明における投票者装置のフローチャートを示す。まず、既存のＷＷＷブラウザ上からサービスを享受するための投票者ＩＤ、パスワードの入力が必要となる（Ｓ１）。取得していれば投票サービスを利用でき、取得していなければ投票者ＩＤ、パスワードの発行申請を行う（Ｓ２）。つまり投票者ＩＤ、パスワードはこのシステム加入資格、つまり選挙権に相当する。投票者ＩＤ、パスワードを入力すれば、暗号化鍵が取得できる（Ｓ３）。次に投票を行う際に必要な投票者の認証書の所持を確認し（Ｓ４）、所持していなければその認証書の発行を申請する（Ｓ５）、所持していればその認証書の選択を行う（Ｓ６）。ここで選択した認証書を用いて投票時に認証者装置へ送信する。つまり認証

書は投票者の本人性を認証するためのもので、認証書は認証局により発行され、本人の氏名又は識別子（ＩＤ）と、公開鍵などを認証局が証明したものであって、投票者装置では、例えばその公開鍵と対応した秘密鍵で乱数Ｒを暗号化し、その暗号化乱数Ｒと認証書を認証者装置へ送り、認証者装置では暗号化乱数を認証書の公開鍵で復号し、復号結果が受信したＲと等しければ、その公開鍵と対応する秘密鍵をもっているものは、その認証書の氏名の者と一致しているとし、本人性の認証を行う。クレジットカードが複数使用されるようにこの認証書も複数の認証局により発行されることがあり、その場合、認証書の選択が必要となる。

【００１７】実際に投票を行う際には、投票毎に必要な投票ＩＤが必要となる。投票ＩＤを取得するために認証者装置に対して投票ＩＤ発行要求を送信する（Ｓ７）、投票ＩＤ発行回答受信を待ち（Ｓ８）、投票ＩＤを入手する（Ｓ９）。すでに投票ＩＤを取得している場合は、前に発行した投票ＩＤを取得する。次に、投票を行うための投票要求（例えば投票用紙の要求）し（Ｓ１０）、その後投票回答（例えば投票用紙）を受信する（Ｓ１１）。次に投票内容を作成し、暗号化処理する（Ｓ１２）。既に投票していれば、前に投じた票内容の確認が送信される。まだ投票していなければ、票を投じることができる（Ｓ１３）。認証者装置からのこの内容でよいかの問合せに対して投票の内容確認を行って（Ｓ１４）、変更がなければ（Ｓ１５）、変更がないという投票内容確認回答処理を行い（Ｓ１６）、変更があればステップＳ１２に戻って改めて投票内容を作り投票し直す。この後、投票期限が過ぎ、投票結果が投票者へ届けられていれば（Ｓ１７）、投票結果の確認を行い（Ｓ１８）、自票の有効性を確認する（Ｓ１９，Ｓ２０）。

【００１８】図４にこの発明における認証者装置のフローチャートを示す。認証者装置は一連の投票サービスに必要な認証書を所持していなければ（Ｓ１）、認証書の発行を申請し（Ｓ２）、所持していれば、その認証書を選択する（Ｓ３）。ここで選択した認証書を用いて各種処理を行う。要求受信を待ち（Ｓ４）、要求受信として投票ＩＤ発行要求を受信すれば（Ｓ５）、投票者と投票ＩＤの表から投票ＩＤの発行の有無を調べ（Ｓ６）、発行していなければ投票ＩＤ発行を行い（Ｓ７）、投票者と投票ＩＤの表にその投票ＩＤを加え、投票ＩＤを投票者装置へ送信する（Ｓ８）。すでに発行していれば以前に発行した投票ＩＤを送信する。また、要求受信が投票要求受信であれば（Ｓ９）、投票の有無を調べ（Ｓ１０）、すでに投票していれば以前に投じた票の内容確認を投票者装置に依頼する（Ｓ１１）、つまりこのような内容でよいかの確認をとる。まだ投票していなければ投票を受け付け（Ｓ１２）、その投票の正当性の認証処理をする（Ｓ１３）。つまり、その投票者が本人であることを同時に受信した認証書を用いる本人性認証により確認し、またその票が投票者本人のものであることを同時に送られた投票ＩＤと投票者との対応が、認証者装置に保持している投票ＩＤと投票者表を参照して確認し、また受信した投票ＩＤによる投票が既に行われていないかにより二重投票でないことを確認する。

【００１９】これら全ての確認に合格すると、その投票の内容の確認を投票者装置に依頼する（Ｓ１１）。投票内容確認回答を投票者装置から受信し、投票内容に変更があれば（Ｓ１４）、ステップＳ１３に戻って認証処理を行い、投票内容に変更がなければその確認済の票を保管しておく（Ｓ１５）。投票期限が経過していれば（Ｓ１６）、保管しておいた票を収集して投票リストの作成を行う（Ｓ１７）。この投票リストを開票者装置へ提供するために、投票リスト投入要求（投票リストを送ってよいかの問合せ）を開票者装置へ送信し（Ｓ１８）、回答を待つ（Ｓ１９）。送ってよいとの回答を受信したら投票リストを開票者装置に配布する（Ｓ２０）。また、要求受信が問合せ要求受信であれば（Ｓ２１）、その問合せ要求を開票者装置へ送り（Ｓ２２）、開票者装置からその問合せ要求に対する問合せ回答を受信すると（Ｓ２３）、その問合せ回答を投票者装置へ返して（Ｓ２４）、ステップＳ４の要求受信の待機状態へと戻る。以上における認証者装置から投票者装置又は開票者装置へ送信する場合はその送信内容に認証書を付加して、これを受信した装置で、間違いなく認証者装置からの受信であること、つまり本人性の認証ができるようにする。

【００２０】図５にこの発明における開票者装置のフローチャートを示す。開票者装置は一連の投票サービスに必要な認証書を所持していなければ（Ｓ１）、認証書の発行を申請し（Ｓ２）、所持していれば、その認証書を選択する（Ｓ３）。ここで選択した認証書を用いて各種処理を行う。まず、投票する際に投票内容に対して施す暗号化鍵を生成し（Ｓ４）、投票者装置に対して配布する（Ｓ５）。その後、要求受信の待機状態となる（Ｓ６）。ここで、要求受信として認証者装置から投票リスト投入要求（投票リストを送信してもよいかの問合せ）を受信すれば（Ｓ７）、投票リスト投入回答（受信準備ができている）を認証者装置へ送信し（Ｓ８）、投票リストを認証者装置から取得する（Ｓ９）。この投票リストに対して開票（復号）を行い、集計し（Ｓ１０）、その投票結果を投票者装置全てに送信する（Ｓ１１）。その投票結果には投票のあった投票ＩＤを付けて投票者が自分の投票ＩＤにより正しく投票がなされたことを確認できるようにされる。また、要求受信が問合せ要求受信であれば（Ｓ１２）、問合せ回答を認証者装置へ返して、ステップＳ６の要求受信の待機状態へと戻る（Ｓ１３）。

【００２１】上述において、自分の票の有効性を知る必要がなければ投票ＩＤを省略してもよい。また票の内容が正しく本人により作成されたものであり、改ざんされ

9

ていないものであることを確認するために、投票者装置で暗号化された投票内容に対してデジタル署名を付加し、この署名の検証を認証者装置で行えばよい。また投票者装置で、投票者の氏名、年令、性別などの個人情報を票と共に認証者装置へ送り、認証者装置で、個人情報中の公開してもよいとされているものを開票者装置へ送れば、投票結果を集計する際に票の項目に対する年令層別、性別などの分布を知る分析データを作成することができる。

【００２２】

【発明の効果】以上述べたようにこの発明によれば、投票者装置と開票者装置の間に仲介者装置として認証者装置を設け、投票者の認証業務を行わせ、投票者の投票内＊

10

＊容を暗号化する鍵を開票者装置が生成し、投票者装置が投票を行う事前に暗号化鍵を渡しておくことにより、投票者以外の者に対して投票者名と投票内容の対応を隠蔽し、投票者のプライバシー保護を確保する効果が得られる。

【図面の簡単な説明】

【図１】この発明の電子投票手順を示す図。

【図２】この発明における各処理を示す図。

【図３】投票者装置の処理手順を示す図。

【図４】認証者装置の処理手順を示す図。

【図５】開票者装置の処理手順を示す図。

【図６】従来の電子投票方法の手順を示す図。

【図１】

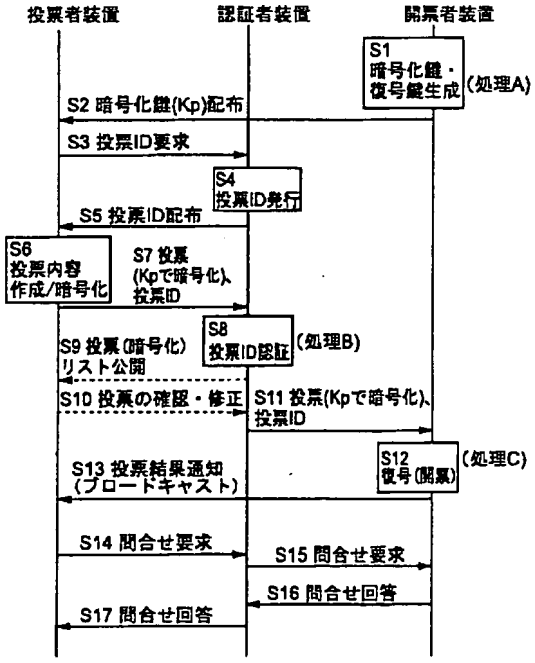

図 1

【図２】

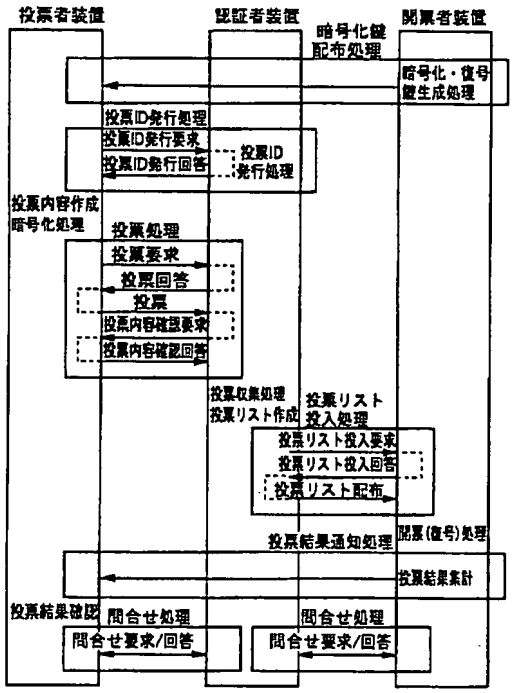

図 2

【図３】

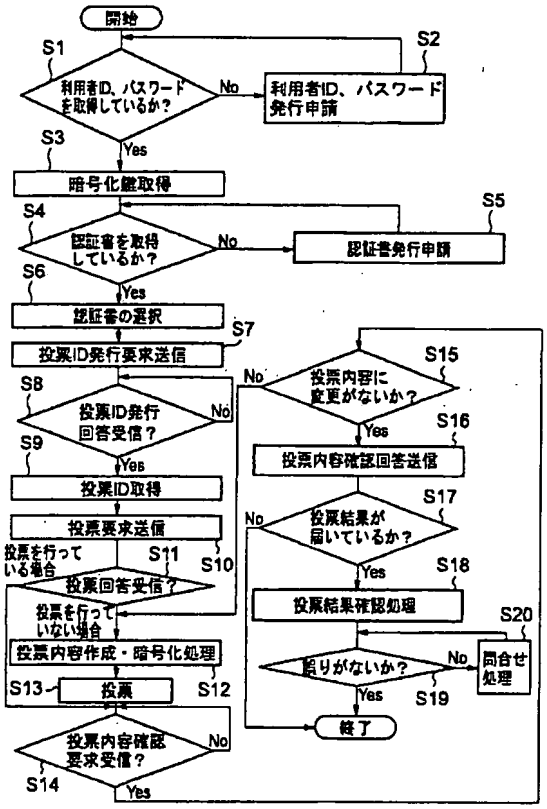

図３

【図４】

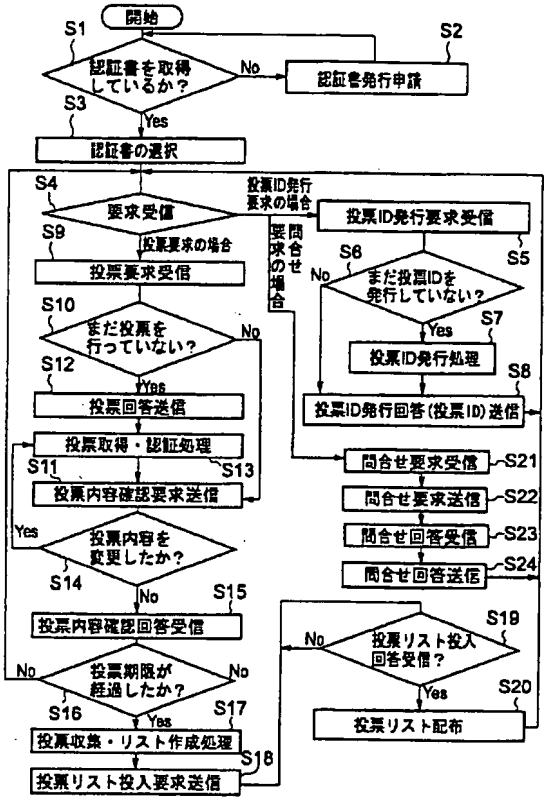

図４

【図６】

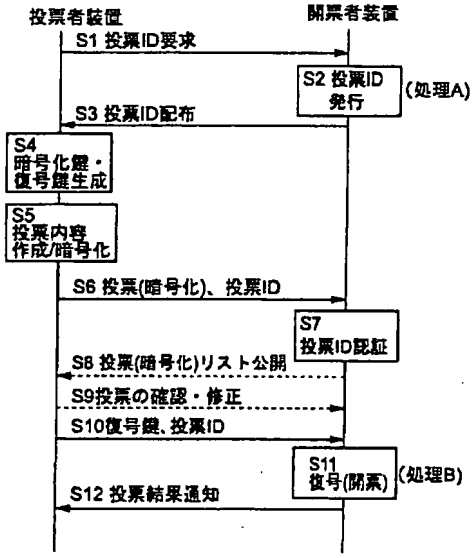

図６

【図５】

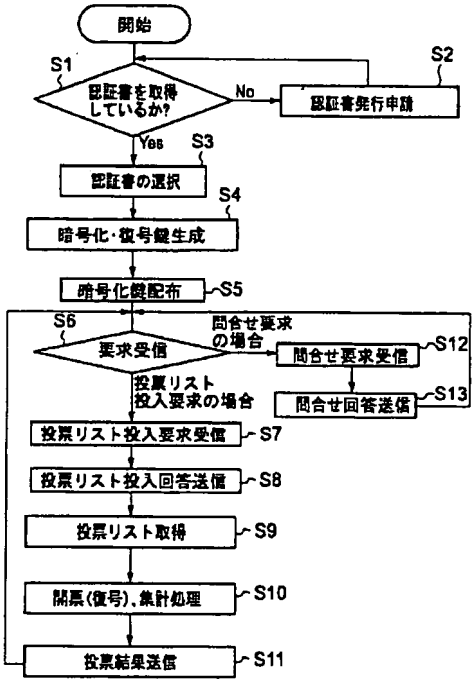

図５

フロントページの続き

Ｆターム(参考) 5B049 AA05 BB36 CC01 EE02 EE23
FF02 GG04 GG07 GG09 GG10
5J104 AA07 EA16 JA21 KA01 KA05
MA01 NA02 NA27 PA17
9A001 CC07 EE03 JJ71 KK56 KK60
LL03

(19) Japan Patent Office (JP)
(12) **Japanese Unexamined Patent Application Publication (A)**

(11) Japanese Unexamined Patent Application Publication Number

2000–269957
(P2000-269957A)
(43) Publication date 29 September 2000 (2000.9.29)

(51) Int. Cl.[7]	Identification symbols	FI			Subject codes (reference)
H 04 L 9/32		H 04 L	9/00	675D	5B049
G 06 F 19/00		G 09 C	1/00	620Z	5J104
G 09 C 1/00	620			640B	9A001
	640	G 06 F	15/28	B	

Request for examination: Not filed Number of Claims: 11 OL (8 pages total)

(21) Application No. H11–73118

(22) Filing date 18 March 1999 (1999.3.18)

(71) Applicant 000004226
Nippon Telegraph and Telephone Corp.
3-1 Otemachi 2-chome, Chiyoda-ku, Tokyo

(72) Inventor Soma, Hiroyuki
c/o Nippon Telegraph and Telephone Corp.
19-2 Nishi Shinjuku 3-chome, Shinjuku-ku, Tokyo

(72) Inventor Tanaka, Hiroki
c/o Nippon Telegraph and Telephone Corp.
19-2 Nishi Shinjuku 3-chome, Shinjuku-ku, Tokyo

(74) Agent 100066153
Patent Attorney Kusano, Takashi (and 1 other)

Continued on last page

(54) {Title of invention} Electronic voting method and program recording medium therefor

(57) {Abstract}
{Problem} To conceal the correspondence between voter name and vote content from persons other than the voter.
{Solution} The ballot opener generates a public key cryptography encryption key and decryption key (S1) and distributes the encryption key to all voters (S2); the voter asks the authenticator to issue a voting ID (S3); the authenticator issues a voting ID to the voter (S4); the voter encrypts the vote content with the encryption key (S6) and sends the encrypted vote and voting ID to the authenticator (S7); the authenticator authenticates the legitimacy of the vote (S8) and sends a list of encrypted votes and voting IDs to the ballot opener (S11); the ballot opener decrypts the encrypted votes with the decryption key, counts the votes, and publishes the voting results together with the voting IDs (S13).

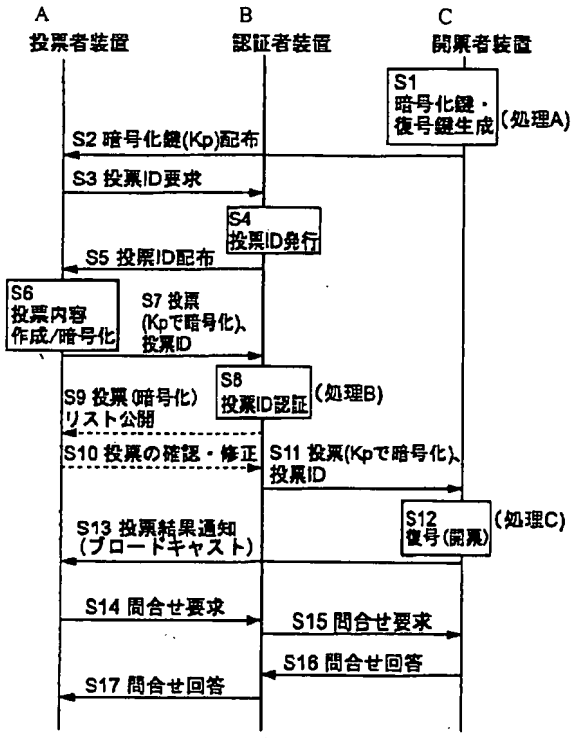

Figure 1

S1: Encryption/decryption key generation (processing A)
S2: Encryption key (Kp) distribution
S3: Voting ID request
S4: Voting ID issuance
S5: Voting ID distribution
S6: Vote content generation/encryption
S7: Vote (encrypted with Kp), voting ID
S8: Voting ID authentication (processing B)
S9: (encrypted) Vote list publication
S10: Confirmation/correction of vote
S11: Vote (encrypted with Kp), voting ID
S12: Decryption (opening of ballots) (processing C)
S13: Voting results notification (broadcast)
S14, S15: Inquiry request
S16, S17: Inquiry response
A: Voter device
B: Authenticator device
C: Ballot opener device

{Scope of patent Claims}

{Claim 1} An electronic voting method using a network, distinguished in that:

a voter device sends the vote to an authenticator device;

the authenticator device confirms the voter's identity, that the vote was cast by the voter in question, and that the vote was not cast in duplicate,

and if all those confirmations are successful, sends the vote send to a ballot opener device; and

the ballot opener device opens the received vote.

{Claim 2} An electronic voting method as described in Claim 1, distinguished in that the ballot opener device generates a public key cryptography encryption key and decryption key and distributes the encryption key to the voter devices;

the voter device encrypts votes and sends them to an authenticator device;

the ballot opener device decrypts the encrypted votes with the decryption key and opens them.

{Claim 3} An electronic voting method as described in Claim 1 or 2, distinguished in that:

the voter device requests issuance of a voting ID from the authenticator device;

the authenticator device responds to that issuance request by issuing a voting ID and distributing it to the user device;

the voter device appends the voting ID to the vote sent to the authenticator device;

the authenticator device appends the voting ID to the vote sent to the ballot opener device;

the ballot opener device publishes the relationship between opened and counted votes and the corresponding voting IDs as the voting results to the voter device.

{Claim 4} An electronic voting method as described in Claims 1 through 3, distinguished in that:

the voter device transmits the vote with personal information such as name, age and sex appended thereto;

the authenticator device attaches that personal information which it is permissible to publish to the vote and sends it to the ballot opener device.

{Claim 5} A recording medium with a program recorded thereon, which causes a voter device computer, in an electronic voting method using a network wherein a voter device casts a vote via an authenticator device to a ballot opener device, to perform:

processing of making a voting ID issuance request to the authenticator device;

processing of acquiring a voting ID from the authenticator device;

processing of generating vote content and encrypting that vote content to generate a vote;

processing of sending that vote to the authenticator device;

processing of receiving a vote content confirmation request from the authenticator device;

processing of performing vote generation processing again if there are any modifications to the vote content; and

processing of sending a vote content confirmation response to the authenticator device if there are no modifications to the vote content.

{Claim 6} A recording medium with a program recorded thereon, which causes an authenticator device computer in an electronic voting method using a network, wherein a voter device casts a vote via an authenticator device to a ballot opener device, to perform:

processing of receiving a voting ID issuance request from a voter device;

processing of issuing a voting ID;

processing of transmitting an issued voting ID to the voter device;

processing of authenticating the legitimacy a received vote;

processing of authenticating the identity of the voter using a received certificate;

processing of authenticating that a received vote was cast by a real voter;

processing of authenticating that a received vote is not a duplicate vote;

processing of collecting votes received within the voting period and generating a list thereof; and

processing of sending the vote list to a ballot opener device.

{Claim 7} A recording medium as described in Claim 6, distinguished in that said processing of authenticating legitimacy comprises:

processing of authenticating the identity of the voter using a received certificate;

processing of authenticating that the received vote was cast by a real voter; and

processing of authenticating that the received vote is not a duplicate vote.

{Claim 8} A recording medium as described in Claim 6 or 7, distinguished in that said program comprises a program which causes said computer to execute:

processing of receiving an inquiry request from said voter device;

processing of transmitting the received inquiry request to the ballot opener device;

processing of receiving an inquiry response from the ballot opener device; and

processing of transmitting the received inquiry response to the voter device.

{Claim 9} Recording medium as described in Claims 6 through 8, distinguished in that said program comprises a program which causes said computer to execute:

after said legitimacy authentication processing, processing of making a vote content confirmation request to the voter device; and

processing of receiving a vote content confirmation response from the voter device.

{Claim 10} A recording medium with a program recorded thereon which causes a ballot opener device computer, in an electronic voting method using a network wherein a voter device casts a vote via an authenticator device to a ballot opener device, to perform:

processing of generating an encryption key and decryption key pair;

processing of distributing said encryption key to the voter device;

processing of acquiring a vote list from the authenticator device;

processing of decrypting the encrypted votes in the vote list and counting the votes; and

processing of publishing the counted voting results.

{Claim 11} Recording medium as described in Claim 10, distinguished in that said program comprises a program which

causes said computer to execute:
processing of receiving an inquiry request from the authenticator device; and
processing of transmitting an inquiry response for the received inquiry request to the authenticator device.
{Detailed description of the invention}
{0001}
{Technical field of the invention} This invention relates to electronic voting methods which, in conducting electronic voting via a network, allow the voter to conceal the correspondence between voter name and vote content from persons other than the voter, including the ballot opener, as well as to program recording media therefor.
{0002}
{Prior art} Electronic voting whereby votes are cast via a network is known. For example, it is used in conducting popularity contests on the internet. Here, the conditions required for use in elections, and the like, where strict precision in electronic voting is necessary, are as follows.
{0003}
1. Votes must be cast only by eligible voters.
2. Duplicate voting is not possible.
3. It is not possible to find out the content of other people's votes.
4. Other people's votes cannot be duplicated.
5. It must be possible to discover if anyone has committed improprieties (forgery or deletion) with vote content.
6. All voters must be able to confirm before end of voting that their vote was valid.
Electronic voting schemes which fulfill these conditions include Schneier's electronic voting protocol. This is performed in electronic voting between two parties, the voter and the ballot opener. The procedure taken when a voter votes is that the ballot opener performs authentication of the voter, judges the legitimacy of the vote and opens the ballot, and reflects the vote content in the count results. Here, since the ballot opener receives the vote directly from the voter, he becomes able to find out the correspondence between voter name and vote content. In this case, the voter's vote content flows over a network, and voters who vote via a network have demands to the effect that the voter's personal ideas, intentions and other such private information not become known to other persons.
{0004} Figure 6 shows a conventional electronic voting scheme. In Figure 6, voting, authentication and ballot opening is performed between two parties, the voter and the ballot opener. First, the voter, in order to vote, sends a notification of desire to vote to the ballot opener (S1). The ballot opener issues and delivers a voting ID to the voter who issued a notification of desire to vote (S2, S3), and the voter who has received a voting ID generates a key pair, which is a public key/private key (S4). Using these keys, the voter generates and encrypts the vote content (S5), and sends it together with the voting ID to the ballot opener (S6). Having received this, the ballot opener performs authentication of the voting ID (S7), generates an encrypted vote list, and publishes it to the voter (S8). The voter confirms the list and if there are corrections or the like, casts the vote again (S9). If the published vote content is adequate, the voter sends the decryption key for opening the ballot of that vote together with the voting ID (S10). Once the vote content has been settled on, after expiration of a specified period of time, the ballot opener decrypts and opens the ballots (S11), and publishes the vote counting results to the voters (S12).
{0005} The distinguishing features of this method are indicated below.
1. A voting ID is given to eligible voters, which serves as an identifier giving them the right to vote (processing S1, S2).
2. The number of times a voter voted is checked by means of the voting ID (processing S7).
3. Encryption is performed on the vote content (processing S4, S5).
{0006} 4. Attacks from third parties are prevented by appending a digital signature and certificate (processing S6, S9, S10).
5. Tracing is enabled by retaining a list of voting IDs and voter names (S2).
6. Legitimacy of the voting is disclosed by presenting voting IDs in the count results (S8, S12).
{0007}
{Problems to be solved by the invention} In the prior art, there was a problem in that the ballot opener could obtain both the voter name and the vote content. Namely, the ballot opener could find out the correspondence between voter name and vote content, and privacy protection could not be provided to the voter. The objective of this invention is to provide an electronic voting method which allows the voter to conceal the correspondence between voter name and vote content from persons other than the voter, including the ballot opener, thereby concealing what he voted for, and which furthermore has the function of preventing and tracing double voting or improper voting, and allows the voter to confirm that his vote was valid.
{0008}
{Means of solving the problem} As a method of achieving the aforementioned objective, in this invention, an authenticator device is provided as an intermediary device between the voter device and ballot opener device, which separates the correspondence between voter name and vote content while authenticating the voter. Furthermore, when an authenticator device is provided, it is necessary to conceal the vote content from the authenticator device in order for the authenticator device to receive a vote from the voter device, so encryption is performed on the vote content which allows the ballot to be opened only by the ballot opener device. The generation of encryption and decryption keys for this purpose is performed by the ballot opener device, while the encryption of the vote is performed by the voter device itself, thereby concealing the vote content from persons other than the voter, except for the ballot opener.
{0009} The voter device receives the key for encrypting the vote from the ballot opener device. The voter device is distinguished in that it has the functions of performing voting ID issuance processing whereby it transmits a voting ID issuance request to the authenticator device to obtain a voting ID which is needed when voting, as a result of which a voting ID issuance response is received and a voting ID is obtained; vote casting processing whereby it acquires a voting ID, generates and encrypts the vote content, transmits a vote casting request to the authenticator device, receives a vote casting reply from the authenticator device, and subsequently transmits the encrypted vote content together with the voting ID to the authenticator device, receives a vote content confirmation request from the authenticator device, and if there are no modifications, transmits

a vote content confirmation response to the authenticator device; voting result notification processing which allows the results of voting and the validity of one's own vote to be confirmed; and inquiry processing regarding the voting results.

{0010} The authenticator device is distinguished in that it has the functions of performing voting ID issuance processing whereby it receives a voting ID issuance request from the voter device, issues a voting ID and as a result transmits a voting ID issuance response to the voter device; authentication processing whereby it receives a voting request from the voter device, replies with a voting response, receives the vote, and confirms the legitimacy of the vote; vote casting processing whereby it transmits a vote content confirmation request to the voter device and receives a vote content confirmation response from the voter device; vote list deposit processing whereby it generates a vote list and transmits a vote list deposit request to the ballot opener device, receives a vote list deposit response from the ballot opener device, and performs vote list distribution to the ballot opener device; and inquiry processing whereby it receives an inquiry request from the voter device, transmits an inquiry request to the ballot opener device, receives an inquiry response from the ballot opener device, and transmits an inquiry response to the voter device.

{0011} The ballot opener device is distinguished in that it has the functions of performing encryption key distribution processing whereby it distributes the encryption key generated by encryption and decryption key generation processing to the voter device; vote list deposit processing whereby it receives a vote list deposit request from the authenticator device, answers with a vote list deposit response, and receives the vote list; voting result notification processing whereby it opens (decrypts) the vote list, counts the votes, and distributes the voting results to the voter devices; and inquiry processing whereby it receives an inquiry request from the authenticator device and transmits an inquiry response to the authenticator device.

Operation

By providing an authenticator device which authenticates the voter as an intermediary device, the ballot opener device becomes unable to discern the voter name, as a result of which the voter's privacy is protected in relation to the ballot opener.

{0012} Furthermore, when an authenticator device is provided, the ballot opener device generates an encryption key and decryption key for the votes. Public key encryption is used as the encryption scheme. Here, the authenticator device distributes the generated encryption key in advance to the voter devices, while keeping the decryption key secret. This allows the voter device to perform encryption on the vote content, allowing the vote content to be concealed from persons other than the voter, except for the ballot opener.

{0013}

{Modes of embodiment of the invention} An outline of the electronic voting method of this invention whereby an intermediary (authenticator device) is provided and the ballot opener device is made the device which generates the key for encrypting vote content is shown in Figure 1. First, the ballot opener device generates an encryption key (public key) and decryption key (private key) (S1) (processing A), and distributes the encryption key Kp to the voter devices (S2). The voter device request a voting ID which is needed when voting from the authenticator device (S3), and the authenticator device issues a voting ID (S4) and distributes it to the voter device (S5). The correspondence between the voting ID and voter device is stored in the authenticator device.

{0014} The voter device uses the encryption key Kp obtained from the ballot opener device to encrypt the vote content (S6) and transmits the encrypted vote and voting ID to the authenticator device (S7). Receiving this, the authenticator device performs voter authentication (S8) (processing B), and if legitimacy of the vote can be established, transfers the vote and its voting ID to the ballot opener device (S11). Here, if required, the authenticator device publishes an encrypted vote list to the voter device and request confirmation of vote content (S9), the voter device confirms the vote content and votes again if there are any modifications (S10). The authenticator device which has received a vote cannot perform improper opening of the ballot since it does not have the decryption key. The ballot opener device, having received a voter device's vote from the authenticator device, opens the ballot using the decryption key (S12) (processing C), and the ballot opening results are communicated to all voter devices via a broadcast (S13) (processing D). If a voter's own voting ID is contained in the vote content in the ballot opening results, it means his ballot was correctly opened; if his voting ID is not contained there, the voter sends an inquiry request to the authenticator device (S14), and the authenticator device sends the inquiry request to the ballot opener device (S15). The ballot opener device sends a response to the inquiry to the authenticator device (S16), and the authenticator device sends that inquiry response to the user device (S17).

{0015} Figure 2 shows the processing involved in the voting process in this invention. First, in the encryption key distribution processing, the ballot opener device generates the encryption key and decryption key for performing encryption on the vote content for the voter devices. The encryption key generated here is distributed to all the voter devices. In the voting ID issuance processing, the authenticator device issues and provides the voting ID needed when voting to the voter device. The vote casting processing is carried out when a vote is actually cast. The vote list deposit processing is executed when the vote list generated from votes collected by the authenticator device is provided to the ballot opener device. Inquiry processing is executed when a voter device makes an inquiry regarding the voting results.

{0016} Figure 3 shows a flow chart of the voter device in this invention. First, it is necessary to obtain the voter ID and password for receiving the service via an existing WWW browser (S1). If they have been acquired, the voting service can be used; if they have not been acquired, a voter ID and password issuance request is made (S2). Namely, a voter ID and password correspond to the qualifications for participating in this system, i.e. to the right to vote. By entering a voter ID and password, an encryption key can be obtained (S3). Next, the possession of a certificate needed for voting is confirmed (S4), and if it is not in possession, issuance of a certificate is requested (S5). If it is in possession, selection of the certificate is carried out (S6). The certificate selected here is used to transmit to the authenticator device when voting. That is, the certificate serves to authenticate

the identity of the voter; the certificate is issued by an authenticating authority and comprises certification by the authenticating authority of the name or identifier (ID) of the voter, as well as his public key and the like. A voter device for instance encrypts a random number R with the secret key corresponding to its public key and sends the encrypted random number R and the certificate to the authenticator device; the authenticator device decrypts the encrypted random number with the certificate's public key, and if the decryption results are equal to the received R, the person holding the secret key corresponding to that public key is considered to match the person with the name on that certificate and his identify is authenticated. Just as multiple credit cards are used, this certificate may also be issued by multiple authenticating authorities, in which case selection of a certificate becomes necessary.

{0017} When actually voting, a voting ID required for each instance of voting becomes necessary. In order to acquire a voting ID, a voting ID issuance request is transmitted to the authenticator device (S7), reception of a voting ID issuance response is awaited (S8), and a voting ID is obtained (S9). If a voting ID has previously been acquired, a previously issued voting ID is acquired. Next, voting request to cast a vote is made (for example, a request for ballot) (S10), and then the voting response is received (for example, a ballot) (S11). Next, vote content is generated and encryption processing is performed (S12). If one has already voted, a confirmation of the previously cast vote content is transmitted. If one has not yet voted, a vote can be cast (S13). A vote content confirmation is made in response to an inquiry as to whether this content from the authenticator device is acceptable (S14), and if there are no modifications (S15), vote content confirmation response processing indicating that there are no modifications is carried out (S16), while if there are modifications, one returns to step S12, generates vote content anew and re-votes. Subsequently, once the voting deadline has expired and voting results have reached the voter (S17), confirmation of voting results is performed (S18), and the validity of one's own vote is confirmed (S19, S20).

{0018} Figure 4 shows a flow chart of the authenticator device in this invention. If the authenticator device does not possess a certificate necessary for the series of voting services (S1), it requests issuance of a certificate (S2), and if does possess one, the certificate is selected (S3). The various types of processing are performed using the certificate selected here. The device waits to receive a request (S4). If the request received is a voting ID issuance request (S5), the device examines whether or not a voting ID has been issued based on a table of voters and voting IDs (S6), performs issuance of a voting ID if none has been issued (S7), adds that voting ID to the table of voters and voting IDs, and transmits the voting ID to the voter device (S8). If one has previously been issued, the previously issued voting ID is transmitted. Furthermore, if the request received is a vote casting request (S9), the device examines whether or not a vote has been cast (S10), and if a vote was already cast, it request the voter device to confirm the content of the previously cast vote (S11), i.e. obtains confirmation if such content is acceptable. If no vote has yet been cast, it accepts a vote (S12), and performs processing to authenticate the vote's legitimacy (S13). Namely, the identity of the voter is confirmed through identity authentication using the certificate that was received at the same time, the vote is confirmed to be the voter's by checking the correspondence between the voter and voting ID sent at the same time against the table of voter IDs and voters maintained by the authenticator device, and the vote is confirmed not to be a duplicate vote by confirming that a vote was not already cast based on the received voting ID.

{0019} If all these confirmations are successful, the voter device is requested to confirm the vote content (S11). A vote content confirmation response is received from the voter device, and if there are any modifications to the vote content (S14), the authenticator device returns to step S13 and performs authentication processing, while if there are no modifications to the vote content, the confirmed vote is stored (S15). Once the voting deadline has expired (S16), the stored votes are collected to generate a vote list (S17). In order to provide this vote list to the ballot opener device, a vote list deposit request (an inquiry as to whether a vote list may be sent) is transmitted to the ballot opener device (S18), and a response is awaited (S19). If a response to the effect that the list may be sent is received, a vote list is delivered to the ballot opener device (S20). Furthermore, if the request received is an inquiry request (S21), that inquiry request is sent to the ballot opener device (S22), and upon receiving an inquiry response to that inquiry request from the ballot opener device (S23), that inquiry response is returned to the voter device (S24), and the authenticator device returns to a request reception standby state of step S4. When performing the above transmissions from the authenticator device to the voter device or ballot opener device, a certificate is appended to the transmission content, allowing the device receiving it to authenticate that it was indeed received from the authenticator device, i.e. to authenticate the sender's identity.

{0020} Figure 5 shows the flow chart of the ballot opener device in this invention. If the ballot opener device does not possess a certificate necessary for the series of voting services (S1), it requests issuance of a certificate (S2), and if does possess one, the certificate is selected (S3). The various types of processing are performed using the certificate selected here. First, the encryption key used on the vote content when voting is generated (S4) and distributed to voter devices (S5). Thereafter, the device enters a request reception standby state (S6). Here, if the request received is a vote list deposit request (an inquiry as to whether a vote list may be transmitted) from the authenticator device (S7), a vote list deposit response (ready to receive) is transmitted to the authenticator device (S8), and a vote list is acquired from the authenticator device (S9). Opening (decryption) of ballots is performed on this vote list and the votes are counted (S10), and the voting results are transmitted to all the voter devices (S11). Voting IDs with which votes were cast are attached to the voting results, enabling the voter to confirm that his vote was cast correctly based on his voting ID. Furthermore, if the request received is an inquiry request (S12), the inquiry response is returned to the authenticator device and the ballot opener device returns to the request reception standby state of step S6 (S13).

{0021} In the above, the voting ID may be omitted if there is no need to find out the validity of one's own vote. Furthermore, in order to confirm that the content of a vote has been correctly generated by the voter himself and has not been forged, a digital

signature may be appended to the vote content encrypted by the voter device, and verification of this signature performed by the authenticator device. Furthermore, if the voter device sends personal information such as name, age and sex together with the vote to the authenticator device and the authenticator device sends the personal information which it is considered acceptable to publish to the ballot opener device, analytical data showing the age differences, sex differences, etc. relating to items on the ballot can be generated when voting results are counted.

{0022}

{Effect of the invention} According to this invention as described above, an authenticator device is provided as an intermediary device between the voter device and ballot opener device and is made to carry out voter authentication tasks, the key for encrypting the voter's vote content is generated by the ballot opener device, and the encryption key is delivered before the voter device performs voting, thereby yielding the effect of concealing the correspondence between voter name and vote content from persons other than the voter and ensuring that the voter's privacy is protected.

{Brief description of the drawings}

{Figure 1} A drawing which shows the electronic voting procedure of this invention.

{Figure 2} A drawing which shows the types of processing in this invention.

{Figure 3} A drawing which shows the processing procedure of the voter device.

{Figure 4} A figure which shows the processing procedure of the authenticator device.

{Figure 5} A figure which shows the processing procedure of the ballot opener device.

{Figure 6} A figure which shows the procedure of a conventional electronic voting method.

{Figure 1}

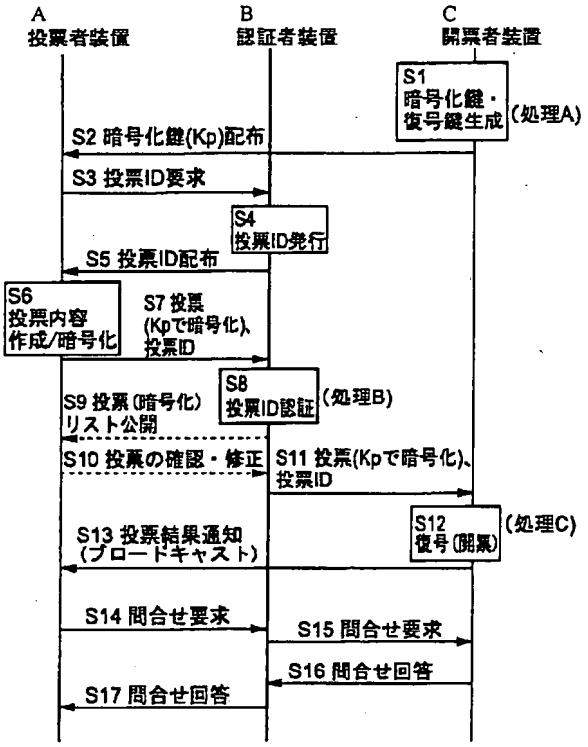

Figure 1

S1: Encryption/decryption key generation (processing A)
S2: Encryption key (Kp) distribution
S3: Voting ID request
S4: Voting ID issuance
S5: Voting ID distribution
S6: Vote content generation/encryption
S7: Vote (encrypted with Kp), voting ID
S8: Voting ID authentication (processing B)
S9: (encrypted) vote list publication
S10: Confirmation/correction of vote
S11: Vote (encrypted with Kp), voting ID
S12: Decryption (opening of ballots) (processing C)
S13: Voting results notification (broadcast)
S14, S15: Inquiry request
S16, S17: Inquiry response
A: Voter device
B: Authenticator device
C: Ballot opener device

{Figure 2}

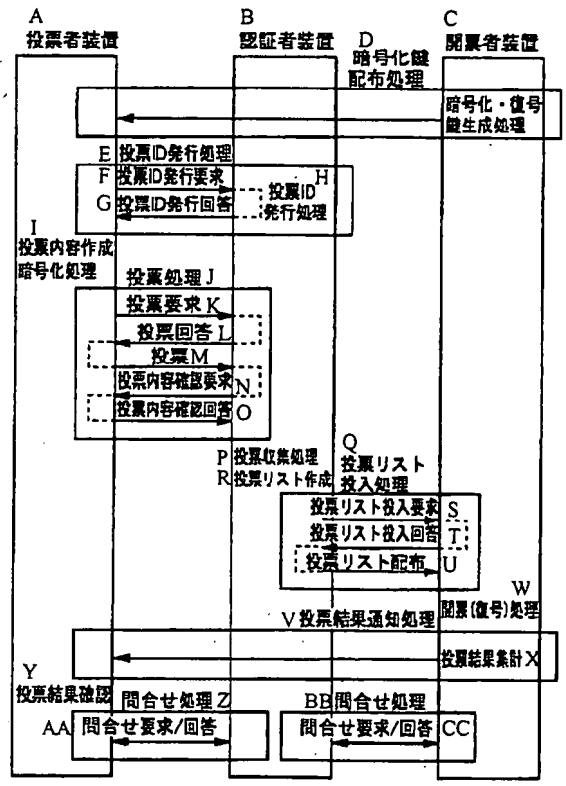

Figure 2

A: Voter device
B: Authenticator device
C: Ballot opener device
D: Encryption key distribution processing
E: Voting ID issuance processing
F: Voting ID issuance request
G: Voting ID issuance response
H: Voting ID issuance processing
I: Vote content generation/encryption processing
J: Vote casting processing
K: Vote casting request
L: Vote casting response
M: Vote casting
N: Vote content confirmation request
O: Vote content confirmation response
P: Vote collection processing
R: Vote list generation
Q: Vote list deposit processing
S: Vote list deposit request
T: Vote list deposit response
U: Vote list distribution
V: Voting results notification processing
W: Ballot opening (decryption) processing
X: Vote results counting
Y: Vote results confirmation
Z: Inquiry processing
AA: Inquiry request/response
BB: Inquiry processing
CC: Inquiry request/response

{Figure 3}

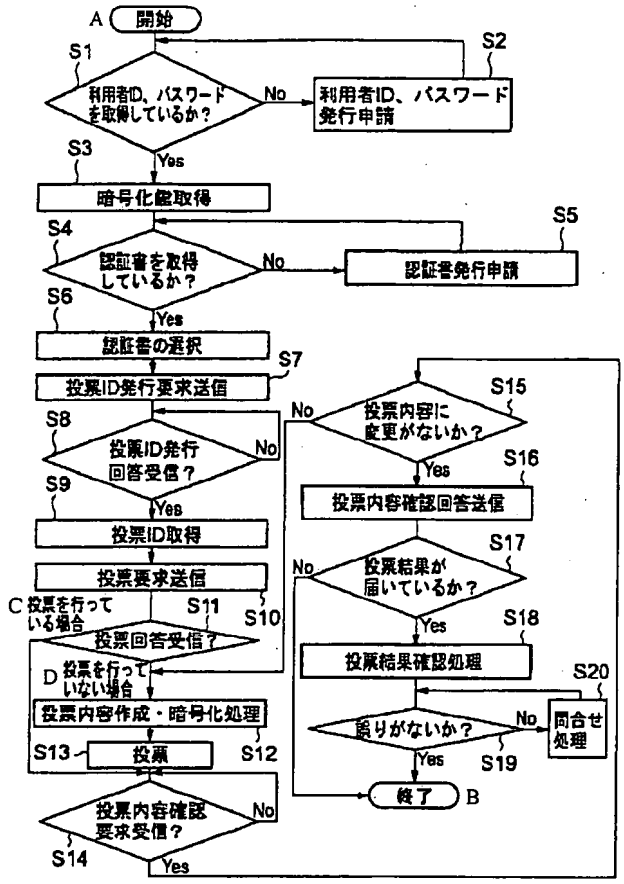

Figure 3

A: Start
B: End
C: Vote has been cast
D: Vote has not been cast
S1: User ID, password acquired?
S2: Request issuance of user ID, password
S3: Acquire encryption key
S4: Certificate acquired?
S5: Request issuance of certificate
S6: Selection of certificate
S7: Transmit voting ID issuance request
S8: Voting ID issuance response received?
S9: Acquire voting ID
S10: Transmit vote casting request
S11: Vote casting response received?
S12: Vote content generation/encryption processing
S13: Cast vote
S14: Vote content confirmation request received?
S15: No modifications to vote content?
S16: Transmit vote content confirmation response
S17: Voting results were delivered?
S18: Voting results confirmation processing
S19: No errors?
S20: Inquiry processing

{Figure 4}

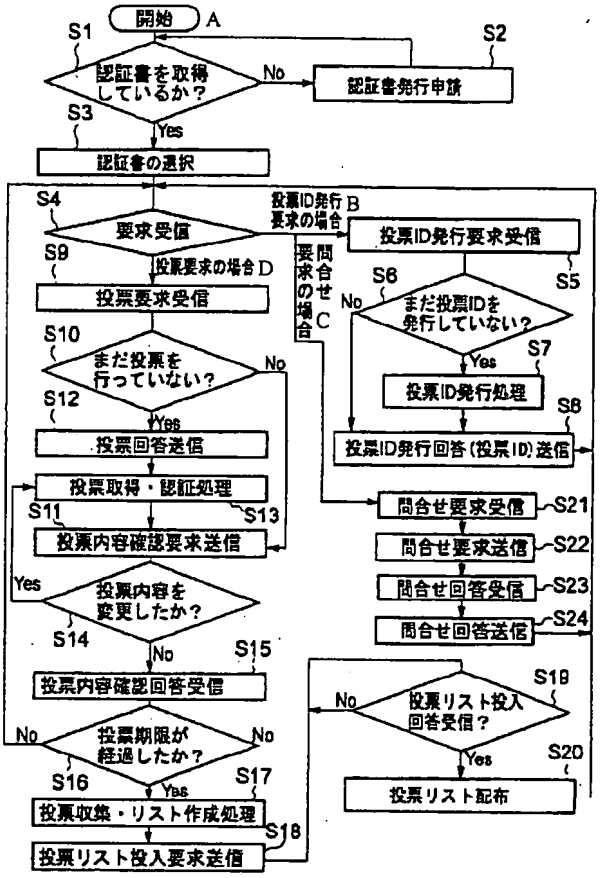

Figure 4

A: Start
B: In case of voting ID issuance request
C: In case of inquiry request
D: In case of vote casting request
S1: Certificate acquired?
S2: Request issuance of certificate
S3: Selection of certificate
S4: Request received
S5: Voting ID issuance request received
S6: Voting ID not issued yet?
S7: Voting ID issuance processing
S8: Transmit voting ID issuance response (voting ID)
S9: Vote casting request received
S10: No vote cast yet?
S11: Transmit vote content confirmation request
S12: Transmit vote casting response
S13: Vote acquisition/authentication processing
S14: Was vote content modified?
S15: Receive vote content confirmation response
S16: Voting deadline expired?
S17: Vote collection/list generation processing
S18: Transmit vote list deposit request
S19: Vote list deposit response received?
S20: Vote list delivery
S21: Receive inquiry request
S22: Transmit inquiry request
S23: Receive inquiry response
S24: Transmit inquiry response

{Figure 5}

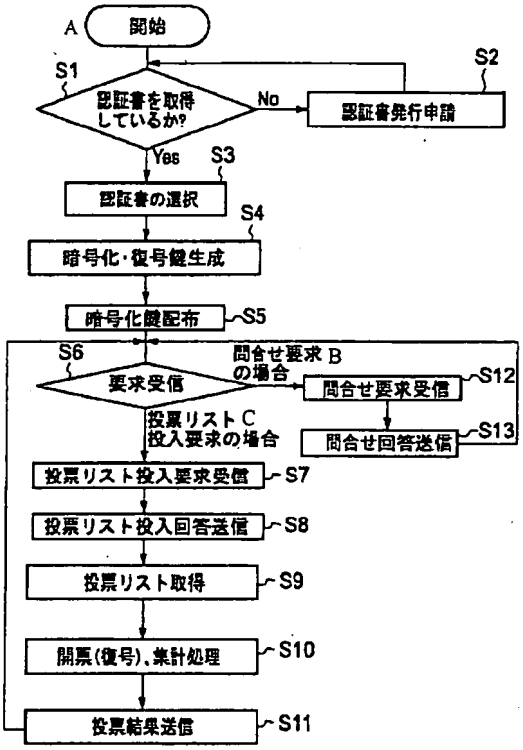

Figure 5

A: Start
B: In case of inquiry request
C: In case of vote list deposit request
S1: Certificate acquired?
S2: Request issuance of certificate
S3: Selection of certificate
S4: Encryption key/decryption key generation
S5: Encryption key distribution
S6: Request received
S7: Vote list deposit request received
S8: Transmit vote list deposit response
S9: Acquire vote list
S10: Ballot opening (decryption), counting processing
S11: Transmit voting results
S12: Inquiry request received
S13: Transmit inquiry response

{Figure 6}

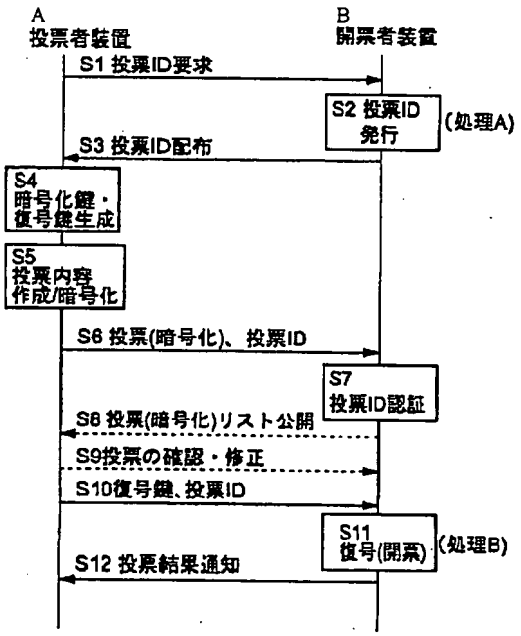

Figure 6

A: Voter device
B: Ballot opener device
S1: Voting ID request
S2: Voting ID issuance (processing A)
S3: Voting ID distribution
S4: Encryption key/decryption key generation
S5: Vote content generation/encryption
S6: Vote (encrypted), voting ID
S7: Voting ID authentication
S8: (encrypted) vote list publication
S9: Vote confirmation/correction
S10: Decryption key, voting ID
S11: Decryption (ballot opening) (processing B)
S12: Voting results notification

Continuation of front page

F terms (reference) 5B049 AA05 BB36 CC01 EE02 EE23
FF02 GG04 GG07 GG09 GG10
5J104 AA07 EA16 JA21 KA01 KA05
MA01 NA02 NA27 PA17
9A001 CC07 EE03 JJ71 KK56 KK60
LL03